SOFTWARE SAFETY DESIGN GUIDELINES

The failure of safety critical functions shall be **detected**, **isolated**, and **recovered** from such that catastrophic and critical hazardous events are prevented from occurring.

Prerequisite conditions (e.g., correct mode, correct configuration, component availability, proper sequence, and parameters in range) for the **safe execution** of an identified hazardous command shall be met before execution.

Software shall provide **error handling** to support safety critical functions.

Software shall provide **fault containment** mechanisms to prevent error propagation.

Software shall provide **proper sequencing** (including timing) of safety critical commands.

Software termination shall result in a **safe system state**.

All safety critical elements (requirements, design elements, code modules, and interfaces) shall be identified as "**safety critical.**"

☑YOUR PREPAREDNESS FOR AN AUDIT OF THE NASA SOFTWARE SAFETY STANDARD WITH THESE SAMPLE AUDIT GUIDE QUESTIONS.

MANAGEMENT:

1. What software has been identified as safety-critical software?
2. Where are software safety non-conformances reported?
3. How are proposed changes evaluated for their impact on system safety?
4. How are all functional software safety requirements and safety-critical software elements verified?
5. What safety program reviews have been conducted to ensure adequate implementation of safety controls?
6. When was the last software safety assurance audit conducted? What were the findings?

GENERAL:

1. Who is the assigned Software Safety Manager?
2. What types of configuration control programs are in place to assure that software safety elements are properly controlled?
3. How aware are project personnel of software safety hazard analysis's and reports?

NASA Office of Safety and Mission Assurance
300 E Street SW
Washington, DC 20024-3210
www.hq.nasa.gov

Publication Date August 29, 2005

NATIONAL AERONAUTICS
AND SPACE ADMINISTRATION
SAFETY AND MISSION
ASSURANCE REQUIREMENTS

NASA-STD-8719.13

Software Safety Standard

Compliance Verification Guide

OFFICE OF SAFETY AND
MISSION ASSURANCE

This brochure is intended to be used as a guide only, not as a replacement for the actual policy. To review Software Safety and Assurance Standards (NASA-STD-8719.13) in its entirety, see http://www.hq.nasa.gov/office/codeq/doctree/texttree.htm.

Explore. Discover. Understand.

Objective of NASA-STD-8719.13:

To provide requirements for software safety and describe the necessary activities to ensure that safety is designed into the software.

Safety Critical Software

"Any software item identified as a potential hazard cause, contributor, control, or mitigation, whether controlled by hardware, software or human operator, is designated as safety-critical, and subjected to rigorous software quality assurance, analysis, and testing. Safety-critical software is also traced through the software safety analysis process until the final verification. Thus, safety critical requirements need to be identified as such to insure future changes, as well as verification processes, take them into appropriate consideration."

Software is safety-critical if it resides in a safety critical system and at least one of the following applies:

- Causes or contributes to a hazard.
- Provides control or mitigation for hazards.
- Controls safety-critical functions.
- Processes safety-critical commands or data.
- Detects and reports, or takes corrective action, if the system reaches a specific hazardous state.
- Mitigates damage if a hazard occurs.
- Resides on the same system (processor) as safety-critical software.

MINIMUM AUDIT POINTS FOR NASA-STD-8719.13

Leadership and Management

- ▶ **Software and System Safety** shall evaluate the software when the system is determined to be safety-critical.
  - ▪ Objective Quality Evidence (OQE) – System Requirements/Software Requirements and Hazard Analysis
- ▶ **Software Safety and Engineering** shall create processes to document, trace, communicate, and close software safety concerns.
  - ▪ OQE – Project Software Safety Requirements Listing/Safety Procedures
- ▶ **Program Manager** shall implement a process or mechanism to document, trace, communicate, and close software safety concerns.
  - ▪ OQE – Software Safety Concerns Process/Safety Plans and Procedures, Hazard Reports, and System/Software Review Records
- ▶ **Software Safety Manager** shall prepare a waiver/deviation package if one or more requirements or certification criteria cannot be met.
  - ▪ OQE – Waiver/Deviation Report and Sign-Off

Core Process

- ▶ **Software Safety**
  - – Shall evaluate hazards for software's contribution to hazard causes, controls, and mitigations.
  - ▪ OQE – Software Hazard Analysis
  - – Shall analyze and report software safety non-conformances to appropriate personnel.
  - ▪ OQE Non-Compliance Reports, Software Hazard Analysis, Configuration Control Board Records
  - – Shall assure that software safety elements are properly controlled.
  - ▪ OQE – Configuration Change Control Records
  - – Shall perform software safety assessment and planning for each software acquisition, maintenance activity, or change to legacy systems.
  - ▪ OQE – Assessment Results, Software Assurance Reports
  - – Shall document software safety planning information in a Software Safety Plan.
  - ▪ OQE – Approved Software Safety Plan
  - – Shall evaluate all software changes for potential safety impact.
  - ▪ OQE – Safety Evaluation Summaries, CCB Records
  - – Shall present the software safety process and results to an appropriate safety panel for certification.
  - ▪ OQE - Evaluations and Assessments, Safety Panel Records
  - – Shall evaluate proposed changes for their impact on system safety.
  - ▪ OQE – Change Proposal Evaluations
- ▶ **Software Configuration Managers** shall perform configuration change control, status accounting, and change verification of safety-critical software requirements and software elements.
  - ▪ OQE – Configuration Change Control Records and Software Hazard Reports
- ▶ **Software Engineering**
  - – Shall identify and assess project tools that could potentially impact safety-critical software and define mitigation strategies, if necessary.
  - ▪ OQE – Assessment and Records
  - – Shall develop software safety requirements and include them in the software requirements specification.
  - ▪ OQE – Requirements Specification
  - – Shall incorporate all functional software safety requirements into the software design.
  - ▪ OQE – Design Specifications

Process Check

- ▶ **Software Assurance**
  - – Shall perform software safety assurance audits.
  - ▪ OQE – Audit Reports
  - – Shall complete all assurance activities prior to acceptance or closure of any software-related system-level hazards.
  - ▪ OQE – Activity Checklist
- ▶ **Software Safety and Assurance Managers** shall plan and conduct safety program reviews to ensure proper implementation of the software safety program.
  - ▪ OQE – Program Review Reports
- ▶ **Safety and Mission Assurance** shall establish a certification process for safety-critical software.
  - ▪ OQE – Certification Process
- ▶ **Software Assurance and Engineering** shall verify that testing and data verification of safety critical software and mitigations are completed before the software is integrated.
  - ▪ OQE – Testing Signoffs